



Defense Information Systems Agency

A Combat Support Agency

NR-KPP Interoperability Testing & Certification

**Joint Interoperability Test Command
9 March 2009**

Agenda

- **DoD / Joint Staff Directives and Instructions**
- **JITC Testing and Certification Process**
- **NR-KPP Elements**
- **Testing Overview**
- **Test Environment**
- **NR-KPP Testing Timeline**
- **Test & Certification Products**

Directives and Instructions

DODD 4630.5

“IT and NSS interoperability shall be verified early, and with sufficient frequency throughout a system’s life ...”

CJCSI 6212.01E

“All IT and NSS must be evaluated and certified for Joint interoperability by **DISA (JITC)**.”

DoD 4630/5000

Interoperability is

“the ability to provide and accept data, information, material, and services ...
...includes both the technical exchange of information and the end-to-end operational effectiveness of that exchange, as required for mission accomplishment.”

DODI 4630.8

“All IT and NSS ... must be tested for interoperability before fielding ... and certified by **DISA (JITC)**.”

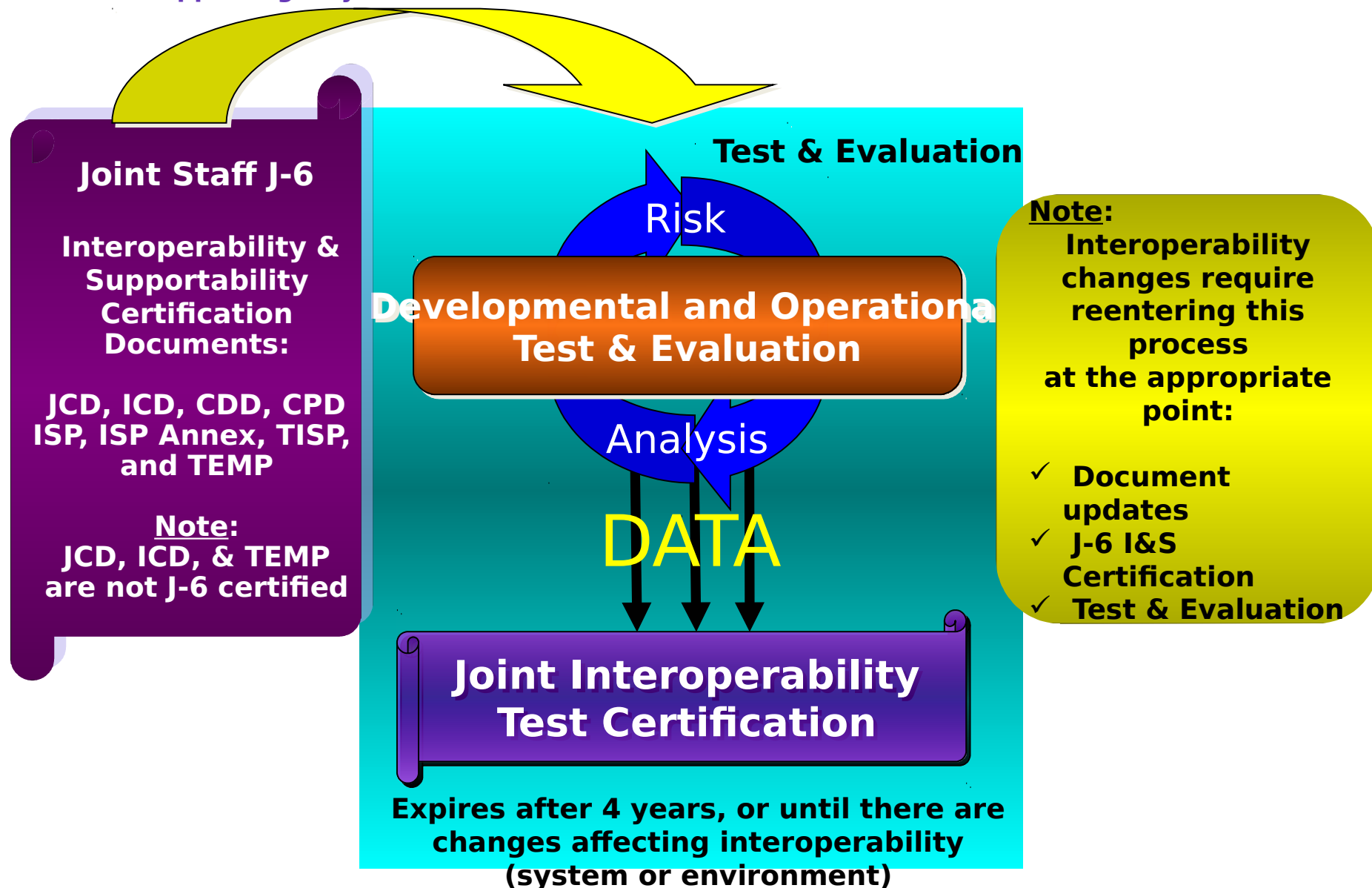
CJCSI 3170.01G

Establishes JCIDS
w/ NR-KPP for
CDD and CPD

DoD 5000 series

“For IT systems, including NSS, .. **JITC** shall provide system interoperability test certification memoranda ... throughout the system life-cycle and regardless of ACAT”

NR-KPP T&E Process



DISAD/E NR-KPP Compliance

A Combat Support Agency



IOP Category	6212.01D NR-KPP	6212.01E NR-KPP	Impact / Interoperability Evaluation
Net-Centricity	Compliance with the Net-Centric Operations and Warfare (NCOW) Reference Model (RM) enterprise services	Compliance with net-centric data and services strategies, DoD IEA	Strengthen NC Data/Service Strategy Compliance <ul style="list-style-type: none"> - Evaluate Data/Service visibility, accessibility, understandability - Evaluate compliance with business rules and principles of DoD IEA
Interfaces / Information Exchanges	Operationally effective information exchanges	Compliant solution architecture products including specified operationally effective information exchanges	Use of DoDAF, JCSFL, Enterprise Architecture, etc. <ul style="list-style-type: none"> - Verify E2E info exchange IAW the solution architecture
Standards Compliance	Compliance with: Global Information Grid (GIG) Key Interface Profiles (KIPs) GIG IT standards and profiles identified in the TV-1	Compliance with GIG Technical Guidance (GTG), including TV-1, GESPs (KIPs until GESPs available)	KIPs transition to GESPs and combined with DISR compliance into GTG element <ul style="list-style-type: none"> - Evaluate applicable GESPs/KIPs via SC/IOP testing - Evaluate standards compliance
IA Compliance	Compliance with DoD information assurance requirements	Compliance with DoD IA requirements	Verification that IA requirements met - no change <ul style="list-style-type: none"> - Verify C&A status - IOP testing is conducted using the approved IA configuration - JITC IA testing where applicable
Supportability	Compliance with Spectrum Supportability and E3, Joint Tactical Radio System (JTRS), Selective Availability Anti-Spoofing Module (SAASM)	Compliance with Spectrum Certification and E3, SAASM, and JTRS requirements	Added Supportability to NR-KPP compliance <ul style="list-style-type: none"> - Verify current DD 1494 (spectrum cert) and E3 compliance - Verify GPS SAASM compliance or waiver - Verify JTRS compliance or waiver

NR-KPP Elements

JITC certifies a system meets *interoperability requirements* contained in the J-6 *certified* NR-KPP (e.g., CPD, ISP/TISP, ISP Annex, NR-KPP Package)

NR-KPP Statement

Solution Architectures

**Net-Centric Data and
Services Strategies**

Technical Standards/Interfaces

**Information
Assurance**

Supportability

Includes descriptions of the system's operation, traceable between the views - defines end-to-end operationally effective information exchange
Describes the activities, standards, and data strategy required to establish, use, operate, maintain, and manage an enterprise-level (EIE MA, COIs) net-centric information environment
Set of managed technical interface standards (DISR/GESPs), bringing visibility and stability to critical interfaces
DIACAP, including availability, integrity, authentication, confidentiality, and non-repudiation

Verify completion of spectrum availability, electromagnetic compatibility, JTRS usage, and GPS SAASM requirements

Testing Overview

Solution Architectures

- **Integrated Architecture products define end-to-end information exchange and use for a given capability.**
 - **Focus is on joint critical exchanges (NR-KPP threshold) and includes all types: automated data and voice.**
 - **MOPs with attributes found in SV-6, e.g., timeliness, throughput, periodicity, size, etc. for assessment of both critical and non-critical exchanges.**
 - **MOEs for determining operational effectiveness and completeness of information exchanges. Use OV-5/6c and SV-5 data to determine if system performance meets operational requirements. Applies to assessment of both critical and non-critical exchanges.**
 - **Interoperability MOPs / MOEs incorporated into TEMP**
 - **Leverage output from PM, OTA, and other COCOM /**

Testing Overview

Net-Centric Data and Services Strategies

- **Identify net-centric services and shared enterprise-level data**
 - Verify services and data are properly registered, visible, and accessible
 - Conformance testing for data / schemata (e.g., proper XML format)
 - During interoperability testing, verify correct provision and use of services / data and any related performance parameters (QoS, timeliness, etc.)
- **Net-centric services / data analyzed by:**
 - COI (may be multiple COIs, overlapping COIs)
 - Design test scenarios to verify effective information exchanges within and among declared COIs
 - EIE MA (Enterprise Info Environment Mission Area - i.e., core services - NCES)
 - Design test scenarios to verify the implementation and use of core services as they become available
- **Core net-centric standards**
 - IPv6 is a net-centric enabling technology that must be considered
 - XML, WSDL, SOAP, UDDI, etc... used to implement SOA via web services

Testing Overview

Technical Standards/Interfaces

- **GESP Declaration (or KIP declaration, e.g., for pre-6212.01E documents) contained in certified CPD, ISP, ISP Annex, TISP, or NR-KPP package, TV-1 from DISROnline.**
 - List of applicable GESPs/KIPs, GESP/KIP profiles, and implementation options, and TV-1 standards
- **JITC reviews applicable standards called out by GESP/KIP/TV-1.**
 - Identify standards/profiles that require testing vs. other evaluation methods.
 - Collect data to support standards conformance certification.
 - Analyze and roll up the results.
- **Information exchanges across key interfaces verified IAW performance parameters during interoperability testing.**
- **Available GESP/KIP/standards information:**
 - DISRonline to select DISR GESP/KIP profiles, TV-1 standards

Testing Overview

Information Assurance

- **During / after DT, JITC will:**
 - **Verify the DIACAP process has been accomplished.**
 - **Review the System Identification Profile (SIP), Certification Report, Plan of Action and Milestones (POA&M) and the IATO, as applicable.**
- **During / after OT, JITC will:**
 - **Review the Comprehensive DIACAP Package.**
 - **Work closely with PMs and OT testers to evaluate IA aspects of the systems.**
 - **Review OT report and verify IA compliance, as appropriate.**
- **Test configuration must mirror approved operational configuration (i.e., testing in a realistic IA environment).**
- **Results of any IA accreditation, waivers, etc. collected for reporting in certification.**

Testing Overview

Supportability

- **Spectrum Supportability:**

- **Spectrum Certification:**

- JITC reports on the stage of the DD 1494.
 - JITC reports on the J/F 12, if the process is complete.

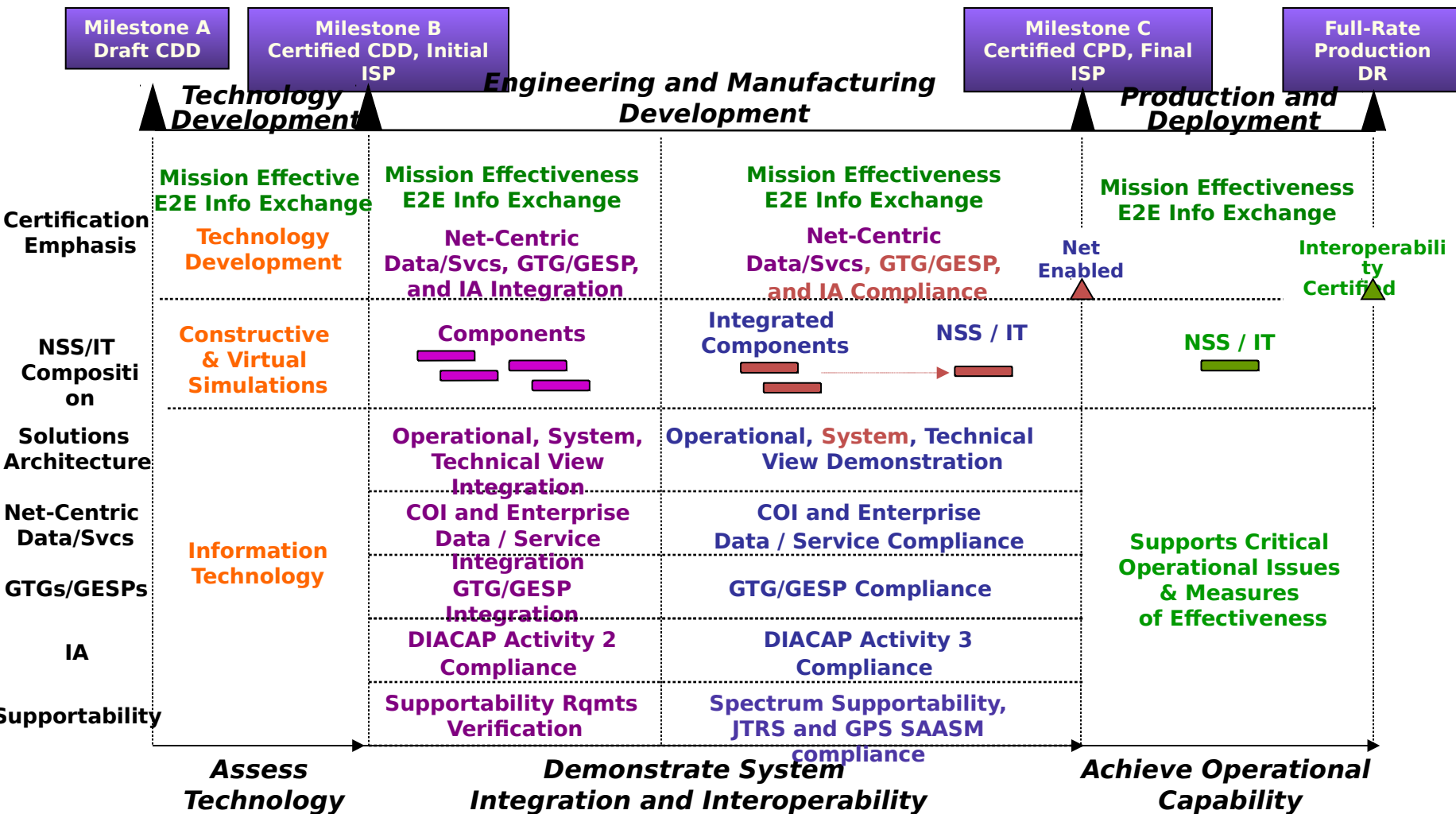
- E3 - JITC reports on E3 control which may include HERO, HERF, HERP, MIL-STD-461 and MIL-STD-464A testing.

- **JTRS** - If the system uses radio-based communications, and the radio is in the 2 MHz to 2 GHz spectrum, and the radio is not JTRS, then JITC will report on the ASD-NII authorization to use a non-JTRS solution.

- **GPS SAASM** - JITC will verify that each JCIDS document, or ISP, TISP, or EISP contains a statement that the program is in compliance with CJCSI 6130.01E, and that analysis of capability technical documentation and test data confirm compliance.

DISA NR-KPP Testing Timeline

A Combat Support Agency



NR-KPP evaluation approach developed before MS

Interoperability Test and Certification

Certification	Description	System can be fielded (Y/N)?
Standards Conformance Certification	System is certified for conformance to a standard/standards profile	No
Joint Interoperability Test Certification	Full system certification. System meets at least <u>all critical</u> interoperability requirements	Yes
Limited Joint Interoperability Test Certification	System meets <u>subset</u> of critical interoperability requirements	Yes, with ICTO
Interim Joint Interoperability Test Certification	A capability module has adequately demonstrated interoperability for at least <u>all critical</u> threshold requirements identified for the increment	Yes
Special Interoperability Test Certification	Based on other J-6 approved requirements (i.e., no NR-KPP) -- E.g., use of UCR for voice switches	Yes
Non-Certification	Critical operational impacts expected Provides a warning to the warfighter	No
Interoperability Assessment	PM would like to determine the interoperability status System may lack J-6 certified	No

Contact Information

- **Hotline**
 - 24/7 C4I Technical Support
 - 1-800-538-JITC (5482)
 - hotline@disa.mil
 - <http://jitc.fhu.disa.mil/support.html>
- **Joint Interoperability Tool (JIT)**
 - <http://jit.fhu.disa.mil>
 - Lessons Learned reports
 - NATO Interface Guide
- **System Tracking Program (STP)**
 - <https://stp.fhu.disa.mil>
 - Test events
 - Test plans and reports
 - Certification results



General Testing Support

(301) 744-2681 or <http://jitc.fhu.disa.mil/gtsform.html>



Questions?



DAU NR-KPP Training

3-hour Program Manager-focused NR-KPP Computer Based Learning module (Net-Ready Key Performance Parameter Course - CLM 029) available online at <http://www.dau.mil>.

Do not need to be a registered DAU student to take module

Lesson Objectives

- **Explain the joint interoperability test and certification process**
- **Explain program managers' responsibilities in joint interoperability testing**
- **Describe the operational and test and evaluation implications of the NR-KPP**
- **Understand the 4-year interoperability re-certification requirement and process**